AMENDMENTS TO THE CLAIMS

1. (Currently amended): An updating system for an encrypted key for a wireless LAN in which a wireless access point is provided on a LAN, said wireless access point being wirelessly connected to a plurality of wireless access terminal devices and in which data is encrypted and transmitted between the wireless access point and the plurality of wireless access terminal devices, said system comprising:

a key management server device, LAN-connected to said wireless access point, comprising:

a storage unit for holding k encrypted keys used in the encrypted communication between said wireless access point and the plurality of wireless access terminal devices, where k is not less than 1; and

an encrypted key generating unit generating said k encrypted keys and storing the generated k encrypted keys in said storage unit;

wherein said key management server device controls said encrypted key generating unit to update one of said encrypted keys stored in said storage unit and delivers the updated encrypted key to said wireless access point and to said plurality of wireless access terminal devices;

wherein each one of said wireless access point and said plurality of wireless access terminal devices decrypts wireless communications using said updated encrypted key.

2. (Previously presented): The updating system for an encrypted key for a wireless LAN as defined in claim 1 wherein:

upon updating said encrypted key stored in said storage unit, said key management server device generates and updates a sole encrypted key at a time by said encrypted key generating unit.

3. (Previously presented): The updating system for an encrypted key for a wireless LAN as defined in claim 1 wherein:

upon updating said encrypted key stored in said storage unit, said key management server device generates a sole encrypted key at a time by said encrypted key generating unit and sequentially updates k encrypted keys stored in said storage unit one-by-one at a preset interval.

4. (Previously presented): The updating system for an encrypted key for a wireless LAN as defined in claim 1 wherein:

where k is greater than 1, said key management server device sequentially updates all except a remaining one of said k encrypted keys stored in said storage unit one-by-one at a preset first interval, said key management server device updating the remaining one key at a second interval which is longer than said preset first interval.

5. (Previously presented): The updating system for an encrypted key for a wireless LAN as defined in claim 2 wherein:

said wireless access point comprises an updating unit updating an nth encrypted key, stored and managed by said wireless access point, on reception of a delivered nth encrypted key updated by said key management server device, where $1 \leq n \leq k$, and where k is greater than 1, and an encryption unit encrypting an encrypted key updating notification message, using an encrypted key other than said nth encrypted key;

each of said plurality of wireless access terminal devices comprising a key generating unit generating an encrypted key updating requesting message on reception of said encrypted key updating notification message from said wireless access point and an encryption unit encrypting said encrypted key updating requesting message, using the same encrypted key as that used in said encrypted key updating notification message; and

said wireless access point also comprising a transmission unit advising said key management server device of reception of said encrypted key updating requesting message;

said key management server device also comprising a verification unit verifying whether or not an encrypted key may be delivered to one of said plurality of wireless access terminal devices on reception of the encrypted key updating requesting message from said wireless access point, and a delivery unit that delivers, if such verification is true, to said wireless access point the encrypted key addressed to said one of said plurality of wireless access terminal devices.

6. (Previously presented): The updating system for an encrypted key for a wireless LAN as defined in claim 2 wherein:

said wireless access point comprises an updating unit updating an nth encrypted key, stored and managed by said wireless access point, on reception of a delivered nth encrypted key updated by said key management server device, where $1 \leq n \leq k$, and an encryption unit encrypting an encrypted key updating notification message, using an initially updated one of k encrypted keys stored and managed by said wireless access point;

each of said plurality of wireless access terminal devices comprising a generator unit generating an encrypted key updating requesting message on reception of said encrypted key updating notification message from said wireless access point and an encryption unit encrypting said encrypted key updating requesting message, using the same encrypted key as that used to encrypt said encrypted key updating notification message;

said wireless access point also comprising a transmission unit advising said key management server device of the reception of said encrypted key updating requesting message;

said key management server device also comprising a verification unit verifying whether or not an encrypted key may be delivered to one of said plurality of wireless access terminal devices on reception of the encrypted key updating requesting message from said wireless access point and a delivery unit that delivers, if such verification is true, to said wireless access point the encrypted key addressed to said one of said plurality of wireless access terminal devices.

7. (Previously presented): The updating system for an encrypted key for a wireless LAN as defined in claim 5 wherein

said wireless access point comprises a generator unit generating an encrypted key delivery message on reception of an encrypted key addressed to said one of said plurality of wireless access terminal devices from said key management server device; and

an encryption unit encrypting said encrypted key delivery message, using an encrypted key other than the nth encrypted key;

said one of said plurality of wireless access terminal devices also comprising an updating unit updating an nth encrypted key stored and managed by

said one of said plurality of wireless access terminal devices on reception of an nth encrypted key by said encrypted key delivery message from said wireless access point.

8. (Previously presented): The updating system for an encrypted key for a wireless LAN as defined in claim 6 wherein

said wireless access point comprises a generator unit generating an encrypted key delivery message on reception of an encrypted key addressed to said one of said plurality of wireless access terminal devices from said key management server device; and

an encryption unit encrypting said encrypted key delivery message, using an encrypted key other than the nth encrypted key;

said one of said plurality of wireless access terminal devices also comprising an updating unit updating an nth encrypted key stored and managed by said one of said plurality of wireless access terminal devices on reception of said nth encrypted key by said encrypted key delivery message from said wireless access point.

9. (Previously presented): The updating system for an encrypted key for a wireless LAN as defined in claim 5wherein:

said wireless access point comprises a generator unit generating an encrypted key delivery message on reception of an encrypted key addressed to said one of said plurality of wireless access terminal devices from said key management server device, and

an encryption unit encrypting said encrypted key delivery message, using an initially updated one of k encrypted keys stored and managed by said wireless access point;

said one of said plurality of wireless access terminal devices also comprising an updating unit updating an nth encrypted key stored and managed by said one of said plurality of wireless access terminal devices on reception of an nth encrypted key by delivered said encrypted key delivery message from said wireless access point.

10. (Previously presented): The updating system for an encrypted key for a wireless LAN as defined in claim 6 wherein:

said wireless access point comprises:

a generator unit generating an encrypted key delivery message on reception of an encrypted key addressed to said one of said plurality of wireless access terminal devices from said key management server device, and

an encryption unit encrypting said encrypted key delivery message, using an initially updated one of k encrypted keys stored and managed by said wireless access point;

said one of said plurality of wireless access terminal devices also comprising an updating unit updating an nth encrypted key stored and managed by said one of said plurality of wireless access terminal devices on reception of an nth encrypted key by delivered said encrypted key delivery message from said wireless access point.

11. (Previously presented): The updating system for an encrypted key for a wireless LAN as defined in claim 1 wherein:

said one of said plurality of wireless access terminal devices comprises means for notifying the wireless access point of a lumped encrypted key updating requesting message on detection of a preset factor;

said wireless access point comprising means for notifying said key management server device of reception of said lumped encrypted key updating requesting message from said one of said plurality of wireless access terminal devices;

said key management server device comprising means for verifying whether or not the encrypted key addressed to said one of said plurality of wireless access terminal devices can be delivered in a lump to said one of said plurality of wireless access terminal devices on reception of said lumped encrypted key updating request from said wireless access point; and

means for delivering encrypted key addressed to said one of said plurality of wireless access terminal devices in lump to said wireless access point if said verifying means has verified that the encrypted key can be delivered in a lump to said one of said plurality of wireless access terminal devices;

said wireless access point also comprising means for generating a lumped encrypted key delivery message on reception in lump of said encrypted keys addressed to said one of said plurality of wireless access terminal devices from said key management server device;

said one of said plurality of wireless access terminal devices also comprising means for updating the encrypted keys stored in said one of said plurality of wireless access terminal devices in lump on reception of said lumped encrypted key delivery message from said wireless access point.

12. (Currently amended): An updating method for an encrypted key for a wireless LAN comprising:

(a) providing a wireless access point provided on a LAN, said wireless access point being wirelessly connected to a plurality of wireless access terminal

devices and in which data is encrypted and transmitted between the wireless access point and the plurality of wireless access terminal devices;

(b) generating, by a key management server device, LAN-connected to said wireless access point, k encrypted keys, k being not less than 1, used for encrypted communication between said wireless access point and said plurality of wireless access terminal devices;

(c) storing and managing, by said key management server device the k encrypted keys;

(d) updating one of the encrypted keys under a preset condition, and

(e) delivering the updated encrypted key to said wireless access point and to said plurality of wireless access terminal devices; and

(f) each one of said wireless access point and said plurality of wireless access terminal devices decrypting wireless communications using said updated encrypted key.

13. (Previously presented): The updating method for an encrypted key for a wireless LAN as defined in claim 12 wherein:

said key management server device in updating said k encrypted keys stored and managed by said key management server updates said k encrypted keys at a rate of one at a time.

14. (Previously presented): The updating method for an encrypted key for a wireless LAN as defined in claim 12 wherein:

said key management server device in updating said k encrypted keys stored and managed by said key management server device sequentially updates said k encrypted keys at a rate of one-by-one at a preset time interval.

15. (Previously presented): The updating method for an encrypted key for a wireless LAN as defined in claim 12 wherein:

where k is greater than 1, said key management server device sequentially updates all except a remaining one key ~~(k—1)~~ of said k encrypted keys stored in and managed by said key management server device one-by-one at a first preset interval, said key management server device updating the remaining one key at a second interval longer than said first preset interval.

16. (Previously presented): The updating method for an encrypted key for a wireless LAN as defined in claim 13 wherein:

said wireless access point has encrypted communication with said plurality of wireless access terminal devices using anotherencrypted key other than an nth encrypted key stored in and managed by said wireless access point, during a period of time since updating of the nth encrypted key stored in and managed by said wireless access point until the another encrypted key is updated next, where $1 \leq n \leq k$.

17. (Previously presented): The updating method for an encrypted key for a wireless LAN as defined in claim 13 wherein:

said wireless access point has encrypted communication with said plurality of wireless access terminal devices, sequentially using each one of k encrypted keys, other than an nth encrypted key stored in and managed by said wireless access point, during a period of time since updating of the nth encrypted key stored in and managed by said wireless access point until next updating of encrypted key, where $1 \leq n \leq k$.

18. (Previously presented): The updating method for an encrypted key for a wireless LAN as defined in claim 13 wherein:

said wireless access point has encrypted communication with said plurality of wireless access terminal devices, using an initially updated one of k encrypted keys stored in and managed by said wireless access point.

19. (Previously presented): The updating method for an encrypted key for a wireless LAN as defined in claim 16 wherein:

said plurality of wireless access terminal devices encrypt communication with said wireless access point, using one of said k encrypted keys, other than the nth encrypted key, stored in and managed by said plurality of wireless access terminal devices.

20. (Previously presented): The updating method for an encrypted key for a wireless LAN as defined in claim 16 wherein:

said plurality of wireless access terminal devices communicate with said wireless access point, sequentially using each one of said k encrypted keys, other than the nth encrypted key, stored in and managed by said plurality of wireless access terminal devices.

21. (Previously presented): The updating method for an encrypted key for a wireless LAN as defined in claim 16 wherein:

said plurality of wireless access terminal devices communicate with said wireless access point, using the last updated one of k encrypted keys stored in and managed by said plurality of wireless access terminal devices.

22. (Withdrawn): An encryption key management system, comprising:

a key management server device, comprising:

an encryption key generating unit, and

an encryption key storage unit that stores k encryption keys generated by said encryption key generating unit;

a wireless access point coupled to said key management server device; and

a plurality of wireless access terminal devices wirelessly coupled to said wireless access point, each of said wireless access terminal devices storing said k encryption keys.

23. (Withdrawn): The encryption key management system of claim 22, wherein one of said plurality of wireless access terminal devices generates and sends a request for a replacement key for one key of said plurality of encryption keys; and

wherein said key management server device sends a first message that is encrypted with another one of said plurality of encryption keys, said first message comprising said replacement key.

24. (Withdrawn): The encryption key management system of claim 23, wherein said request comprises identifying information of said one of said plurality of wireless access terminal devices and wherein said key management server verifies said identifying information.

25. (Withdrawn): The encryption key management system of claim 22, further comprising an open key encryption messaging protocol employed by said key management server device, said wireless access point, and said plurality of wireless access terminal devices, and wherein said key management server sends a second message comprising said plurality of encryption keys, and wherein said second message is encrypted by said open key encryption messaging protocol.